Cybersecurity (MS)

Master's degree in Cybersecurity at the University of Oregon aims to equip students with comprehensive knowledge and skills in safeguarding digital information and infrastructure. Students will engage in rigorous coursework and hands-on projects that address current cybersecurity challenges, such as network security, cryptography, and risk management.

The program's focus is to develop professionals who can anticipate, identify, and mitigate cyber threats in diverse organizational contexts. Learning objectives include mastering advanced cybersecurity techniques, understanding legal and regulatory frameworks, and developing strategic problem-solving skills. Graduates will earn a Master of Science (MS) degree in Cybersecurity, preparing them for leadership roles in both the private and public sectors, where their expertise will be crucial in protecting critical digital assets.

Program Learning Outcomes

Upon successful completion of this program, students will be able to:

- Understand Fundamental Security Concepts: Gain essential knowledge and up-to-date techniques in cybersecurity, including fundamental security concepts and principles, applied cryptography, program security, and system and network security.
- Develop Hands-on Skills: Hone hands-on skills through computer and network security lab courses and security operation studies.
- Design and Implement Solutions: Draw on broad knowledge and hands-on skills to design, implement, and test solutions to cybersecurity tasks.
- Interdisciplinary Understanding: Understand the wide-ranging effects and interdisciplinary aspects of cybersecurity while attaining proficiency in one or multiple subdomains within the field.
- Apply Foundational Knowledge: Apply and expand foundational knowledge and skills to new problem domains and emerging technologies.
- Effective Communication: Possess effective communication and collaboration abilities, expressing ideas clearly and concisely both orally and in written form.
- Ethical Decision-Making: Adhere to ethical principles and make well-informed decisions in the field of cybersecurity.

Cybersecurity Major Requirements

Grading related criteria for MS in Cybersecurity will mirror the Computer Science policies for MS in Computer Science.

Code	Title	Credits
Depth Courses		
CS 532	Introduction to Networks	4
CS 533	Computer and Network Security	4
CS 534	Computer and Network Security II	4
CS 536	Secure Software Development	4
CS 537	Computer and Network Security Practicum	4
Breadth Courses		
CS 621	Algorithms and Complexity	4
CS 670	Data Science	4
CS 630	Distributed Systems	4
Writing Course		
CS 640	Writing in Computer Research	2
Elective Courses		**20**
Select 5 of the following (20 credits)		
CS 503	Thesis [1]	
CS 551	Database Processing	
CS 571	Introduction to Artificial Intelligence	
CS 572	Machine Learning	
CS 604	Internship: [Topic] [2]	
CS 632	Computer Networks	
CS 633	Advanced Network Security	
CS 510	Experimental Course: [Topic]	
Total Credits		**54**

[1] A maximum of 12 credits is allowed.

[2] A maximum of 4 credits is allowed for CS 604 Internship, and a maximum of 12 credits for CS 604 Internship: Co-op.